Secret Sharing

Henning Hontheim

10. März 2020

Inhaltsverzeichnis

Allein aus Gründen der Lesbarkeit wird auf die gleichzeitige Verwendung mehrerer geschlechtsspezifischer Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten für alle Geschlechter.

1 Wozu Secret Sharing?

Arbeiten Sie mit Anderen an einem geheimen Projekt, so gibt es einige Herausforderungen zu meistern. Was passiert, wenn Sie Ihren Schlüssel der verschlüsselten Daten verlieren? Haben nur Sie einen Schlüssel? Wahrscheinlich nicht. Es ist nützlich, seien es in einem Tresor verschlüsselte Daten, oder die privaten Schlüssel in einer PKI, wenn nicht nur Sie den einzigen Schlüssel besitzen.

Aber wie teilen Sie den Zugriff auf die Daten? Wenn Sie Ihren Schlüssel vervielfältigen würden, hätte ein Einzelner Vollzugriff. Es wäre besser, wenn es mehrere Personen benötigen würde, um Zugriff zu erhalten – idealerweise mehr als die Hälfte aller Beteiligten. Doch wie lässt es sich in der Praxis umsetzen, dass es mehrere Personen benötigt um einen privaten Schlüssel zu rekonstruieren?

Ich möchte hier eine Technik vorstellen, die es erlaubt, Geheimnisse mit anderen zu teilen – das Secret Sharing. Siehe [1] und [3].

1.1 Ein kombinatorisches Beispiel

Mehrere Wissenschaftler N arbeiten zusammen an einem Geheimprojekt. Um die Dokumente geheim zu halten und um Missbrauch vorzubeugen, verschließen sie diese in einem Tresor. Nur wenn mindestens die Hälfte aller Wissenschaftler anwesend ist, soll sich der Tresor öffnen lassen. Wie viele paarweise verschiedene Schlösser S muss der Tresor mindestens besitzen? Wie viele paarweise verschiedene Schlüssel s muss jeder Wissenschaftler mindestens bei sich tragen? Siehe [3] nach [2].

Beispiel 1.1. Sei $N = 11$ die Anzahl aller Wissenschaftler und $n = \left\lceil \frac{N}{2} \right\rceil = 6$ die Anzahl derer, die mindestens anwesend sein müssen, damit sich der Tresor öffnen lässt. Folglich muss es also für jede Teilmenge mit k Wissenschaftlern, wobei $k = N - n = 5$, genau ein Schloss geben, für das keiner der k Wissenschaftler einen Schlüssel besitzt. Also muss der Tresor $S = \binom{N}{k} = \binom{11}{5} = 462$ paarweise verschiedene Schlösser besitzen.

Sei $W = \{w_1, w_2, \ldots w_k, w_{k+1}\}$ mit $|W| = k + 1 = 6$ die Menge von Wissenschaftlern, die mindestens benötigt wird, um den Tresor zu öffnen. Dann gibt es genau ein bestimmtes Schloss S', für das keiner der Wissenschaftler aus $W \setminus w_{k+1}$ einen Schlüssel besitzt, der Wissenschaftler w_{k+1} jedoch schon. Da für jede Permutation von $k = 5$ Wissenschaftlern genau der w_{k+1} existiert, der die Teilmenge W „vervollständigt“, bekommt jeder Wissenschaftler $s = \binom{N-1}{|W|-1} = \binom{N-1}{k} = \binom{10}{5} = 252$ Schlüssel. Das ergibt eine Gesamtanzahl an $11 \cdot 252 = 2772$ Schlüsseln. Dass dies keine praktikable Lösung des Problems ist, ist offensichtlich.

2 Primitives Secret Sharing

2.1 Aufsplitten des Secrets

Ein primitives Vorgehen zur Aufteilung eines Geheimnisses wäre es, dieses nach einer gewissen Anzahl Stellen zu trennen.

Beispiel 2.1. Sei $D = 14561237$ das Geheimnis, welchen unter 2 Personen aufgeteilt werden soll. Bei 8 Stellen, könnte man der ersten Person P_1 die ersten 4 Stellen, der zweiten Person P_2 die letzten 4 Stellen zuteilen.

$$D = 14561237 = \underbrace{1\,4\,5\,6}_{=:D_1}\underbrace{1\,2\,3\,7}_{=:D_2} = D_1 \cdot 10^4 + D_2$$

Der entscheidende Nachteil hierbei ist, dass die Shares[1] D_1 und D_2 Aufschluss über die Beschaffenheit von D geben. Wer D_1 besitzt braucht nur 10^4 Kombinationen zu testen, wohingegen ein unbeteiligter Dritter 10^8 ausprobieren müsste.

Fortan fordern wir also, dass es eine wichtige Eigenschaft der Shares sein muss, keine Informationen über das Geheimnis D preiszugeben, und alle Möglichkeiten von D gleich wahrscheinlich sein sollen.

2.2 One-Time-Padding

Ein Verfahren, welches die geforderte Eigenschaft nicht verletzt, ist das sogenannte One-Time-Padding. Hierbei wird eine zufällige Zahl r zu unserem Geheimnis D addiert, die beide die gleiche Stellenanzahl haben müssen.

Beispiel 2.2. Sei wieder $D = 14561237$ und ein $r_1 = 81613241$ zufällig gewählt. Nun berechnen wir $r_2 = D \oplus r_1$, wobei wir hier $\oplus$ die Addition ist, die Überträge vernachlässigt.

$$\begin{array}{rll} & 14561237 & = D \\ \oplus & 81613241 & = r_1 \\ \hline & 95174478 & = r_2 \end{array} \tag{1}$$

Nun können wir das Geheimnis rekonstruieren, wenn wir $D = r_2 \ominus r_1$ stellenweise rechnen. Unsere Subtraktion $\ominus$ ignoriert auch hier wieder für jede Stelle den (negativen) Übertrag. Somit wäre beispielsweise $1 \ominus 6 = +5$.

$$\begin{array}{rll} & 95174478 & = r_2 \\ \ominus & 81613241 & = r_1 \\ \hline & 14561237 & = D \end{array} \tag{2}$$

[1] Shares sind die Bestandteile eines Geheimnisses, die zur Rekonstruktion dessen an die beteiligten Personen aufgeteilt werden

Wenn wir nun zwei Personen haben, die D unter sich aufteilen möchten, erhält P_1 den Share $r_1 = 81613241$ und P_2 den Share $r_2 = 95174478$. Beide Shares geben keinerlei Aufschluss über die Beschaffenheit von D. Zusammen können P_1 und P_2 das Geheimnis jedoch rekonstruieren.

Beispiel 2.3. Ein weiteres Beispiel

Wie sieht das Ganze jedoch aus, wenn sich mehr als zwei Personen ein Geheimnis teilen möchten? Auch dies ist möglich für eine beliebige Anzahl N an Personen. Doch was passiert, wenn einer der Beteiligten den eigenen Share verliert? Da alle Shares benötigt werden um D zu rekonstruieren, ist das unser SPOF[2]. Da dies in der Praxis für große N sehr schnell zu einem Problem führen kann, möchten wir dieses Verfahren hier nicht länger behandeln.

3 Shamir's Secret Sharing

Blah

3.1 $(2, n)$-Schema

Blah

3.2 $(3, n)$-Schema

Blah

3.3 Allgemeine (k, n)-Schemata

Blah

3.4 Shamir's Secret Sharing $x \bmod p$

Blah

4 Weitere Verfahren

Blah

[2]Single Point of Failure

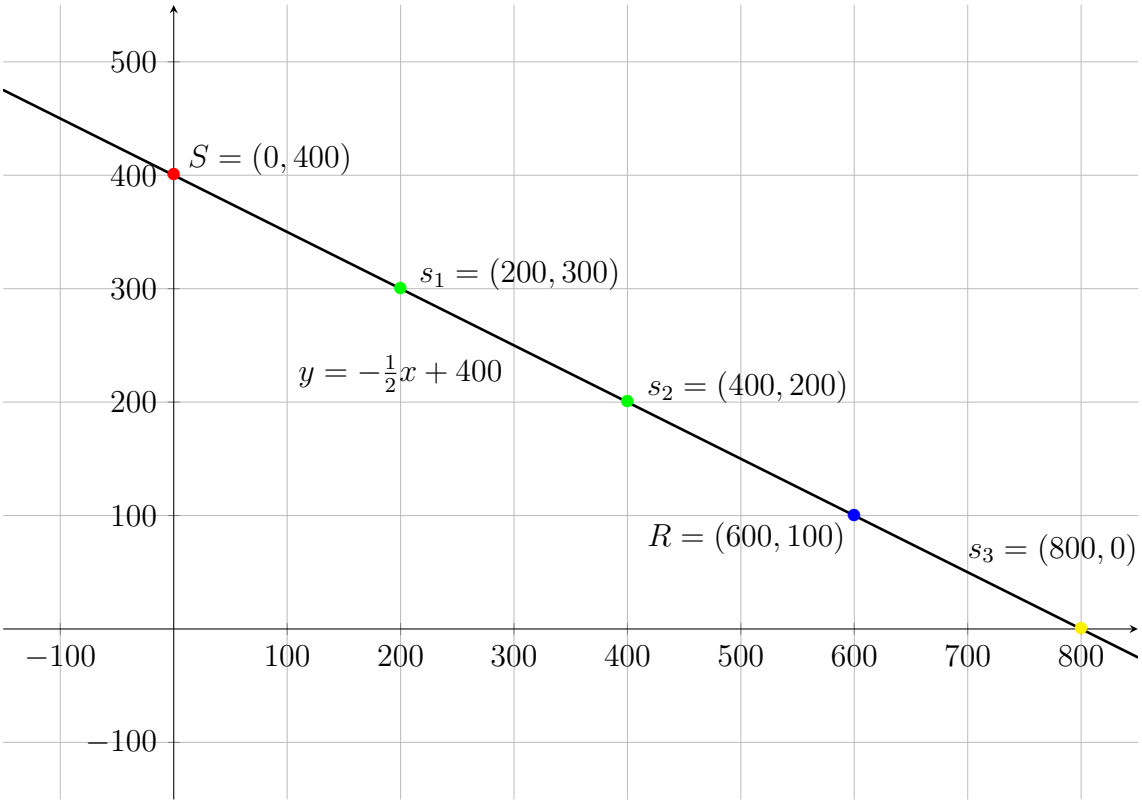

Abbildung 1: Erweiterung des Geheimnisses S als Gerade f für zwei Shares s_1 und s_2.

4.1 Blakeley's

Blah

4.2 whatever...

Blah

5 Fazit

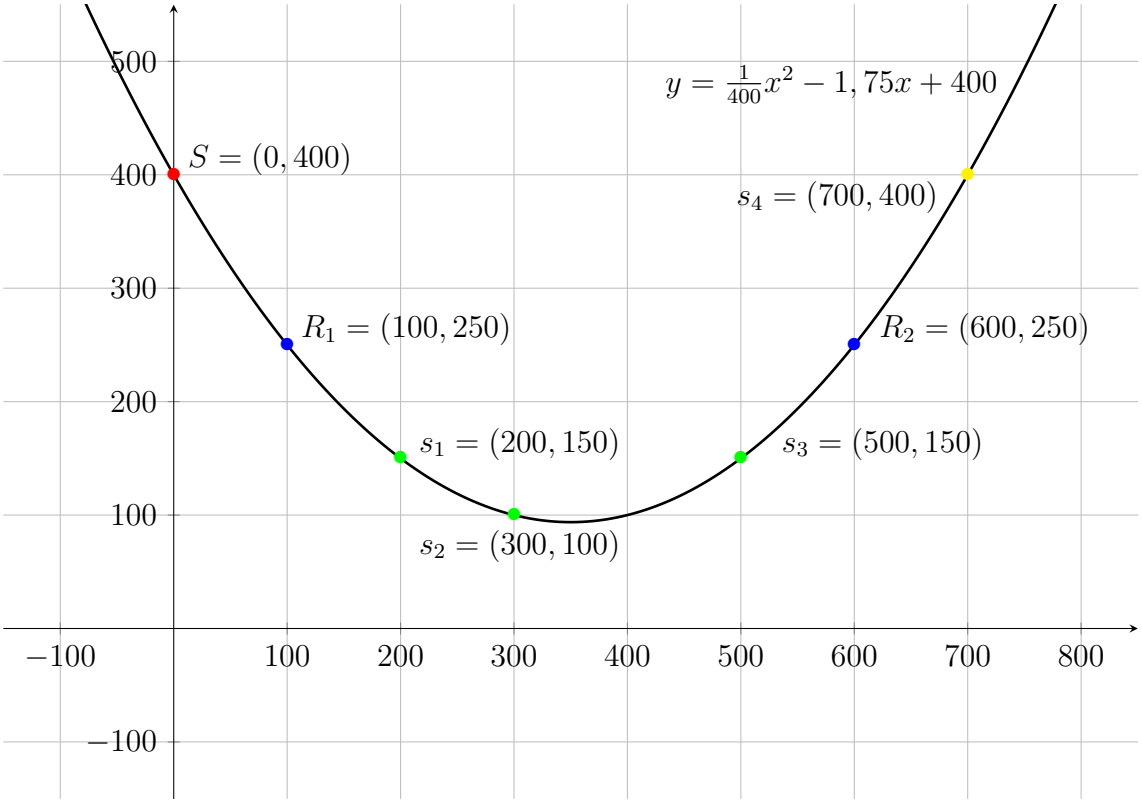

Abbildung 2: Parabel

Abbildungsverzeichnis

Literaturverzeichnis

[1] Buchmann, J. *Einführung in die Kryptographie.* Springer Berlin Heidelberg, 2016.

[2] Liu, C. L. *Introduction to Combinatorial Mathematics.* McGraw-Hill, New York, 1968.

[3] Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (Nov 1979), 612–613.